UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, vs. ERIC DON STANDEFER, Defendant.	CASE NO. 06-CR-2674-H ORDER DENYING MOTION TO SUPPRESS EVIDENCE

On June 4, 2007, defendant Eric Don Standefer ("Defendant") filed a motion to suppress evidence seized from his home. (Doc. No. 22.) On July 16, 2007, the Government filed an opposition to Defendant's motion to suppress evidence. (Doc. No. 24.) On July 19, 2007, Defendant filed a reply. (Doc. No. 25.)

On July 23, 2007, the Court held a hearing regarding Defendant's motion to suppress evidence. Attorney Scott C. Williams appeared for Defendant at the hearing and Assistant United States Attorney Anne Perry appeared for the Government. The Court submitted the motion and ordered that supplemental briefing be filed.

On July 30, 2007, the Government filed a supplemental response in opposition to Defendant's motion to suppress evidence. (Doc. No. 27.) On August 6, 2007, Defendant filed a supplemental reply brief. (Doc. No. 28.) For the following reasons, the Court **DENIES** Defendant's motion to suppress evidence seized from his home.

/ / /

Background

During the course of his duties, Special Agent ("SA") Wade Luders from the San Jose Resident Agency of the San Francisco Field Division of the Federal Bureau of Investigation ("FBI"), identified four internet websites located outside of the United States offering downloadable videos and images of child pornography with a paid subscription. (U.S.' Resp. Opp. Def.'s Mot. Suppress Evidence ("Gov't Opp."), Ex. 1 at 3:13-19.) SA Luders determined that these websites accepted payment via e-gold Ltd. ("e-gold"), a company which allows the instant transfer of gold ownership between users utilizing the internet. (Id. at 1:9-2:5, 3:20-21.) SA Luders selected e-gold as the payment option on one of the pornography websites, which opened an "e-metal Payment Order Form" located on e-gold's website and contained the child pornography site's e-gold account number. (Id. at 3:21-28.) A similar process allowed SA Luders to determine the account numbers of all four websites, which were 2974856, 2973774, 2981290, and 2979416. (Id. at 4:9, 8-13.)

On March 15, 2006, SA Luders served an FBI administrative subpoena upon e-gold, requesting account profile information for the four identified accounts, the transaction history for those accounts, any information on any other accounts owned or controlled by the individuals utilizing the accounts, and any counteraccount profile information for the individuals utilizing the accounts. (Id. at 4:10-14; U.S.' Suppl. Resp. Opp. Def.'s Mot. Suppress Evidence, Ex. 1.) E-gold identified the owners of the accounts by their e-mail addresses, including identifying bucks@keybill.biz as the owner of account number 2981290. (Gov't Opp. at 4:14-18.) E-gold also identified twenty-three other e-gold accounts registered to the same e-mail address, including account numbers 2842101 and 2879936. (Id. at 4:18-21.)

SA Luders determined that account numbers 2842101 and 2879936 received three payments from account number 2907256:

- On February 25, 2006, at 1:23:43 a.m. Eastern Standard Time, the holder of e-gold account number 2907256 purchased a subscription from 2842101 for

$40.00. The e-gold memo filed for the transaction stated "Membership purchase for REALLOLA issue #1." The Internet Protocol ("IP") address utilized to make the E-GOLD payment was 66.167.118.225.

- On February 28, 2006, at 7:53:19 p.m. Eastern Standard Time, the holder of e-gold account number 2907256 purchased a subscription from 2879936 for $50.00. The e-gold memo filed for the transaction stated "WTSS-basic012: SPYCAM LOLITA: direct." The IP address utilized to make the e-gold payment was 66.167.118.14.
- On March 5, 2006, at 1:22:03 a.m. Eastern Standard Time, the holder of e-gold account number 2907256 purchased a subscription from 2879936 for $45.00. The e-gold memo filed for the transaction stated "CHL-basic002:MY LITTLE SISTERS: direct." The IP address utilized to make the e-gold payment was 66.167.118.14.

(Id. at 4:20-5:12.)

SA Luders discovered that the registrant for IP addresses 66.167.118.225 and 66.167.118.14 was Covad Communications Company ("CCC") utilizing the "whois" look-up tool provided by the American Registry of Internet Numbers, which is publicly accessible. (Id. at 5:13-17.) CCC is partnered with Earthlink to provide broadband internet services to residential customers. (Id. at 5:17-19.) On March 29, 2006, the San Jose FBI caused an administrative subpoena to be served upon Earthlink, requesting subscriber information for the 66.167.118.225 and 66.167.118.14 IP addresses during the specific dates and times of the e-gold transactions. (Id. at 5:19-23.) All three IP addresses for the given dates and times were in use by Earthlink subscriber Eric Standefer, address 6212 Stanley Avenue, San Diego, California, telephone number (619) 582-8591, e-mail address onomatopoetic@earthlink.net. (Id. at 5:23-27.)

On May 16, 2006, San Diego FBI Special Agent Travis Johnson conducted a criminal history check on Standefer. (Mem. P. & A. Supp. Mot. Suppress Evidence,

Ex. A at ¶ 22.) SA Johnson discovered that Standefer had no criminal history, but that he was a credentialed school employee for approximately eight years. (Id.) SA Johnson subsequently queried the California Commission on Teacher Credentialing website and discovered that Standefer was authorized to teach "music and cross-cultural, language and academic development emphasis." (Id. ¶ 23.) On May 17, 2007, SA Johnson verified via the San Diego Unified School District website that as of May 2006 Standefer was employed as a music teacher at Jean Farb Middle School. (Id. ¶ 24.) On June 29, 2006, SA Johnson subscribed and swore out an affidavit to a magistrate judge in support of a request for a warrant to seize any and all computers located at 6212 Stanley Avenue, San Diego, California, in order to allow a computer expert to search for evidence of violations of 18 U.S.C. § 2252.[1] (Id. ¶¶ 1-36.)

Plaintiff now moves to suppress the evidence obtained pursuant to the warrant obtained on the basis of SA Johnson's affidavit. Plaintiff argues that the evidence discussed in the affidavit that supported the search warrant was illegally obtained in violation of the Fourth Amendment, and that without that illegally obtained evidence, the Government lacked probable cause to obtain the warrant. Plaintiff also argues that even if the evidence referenced in SA Johnson's affidavit was lawfully obtained, the affidavit failed to raise probable cause to support the warrant. Therefore, Plaintiff argues, all evidence obtained as a result of the warrant must be excluded.

Discussion

I. Standing

The Government argues that the Court should deny Plaintiff's suppression motion because Plaintiff lacks standing to challenge the legality of the evidence obtained pursuant to the administrative subpoena issued to e-gold. To establish standing to challenge the legality of a search or seizure, a defendant must demonstrate

[1] 18 U.S.C. § 2252 outlaws certain activities relating to material involving the sexual exploitation of minors.

that he had a legitimate expectation of privacy in the items seized or the area searched. See United States v. Sarkisian, 197 F.3d 966, 986 (9th Cir. 1999). To demonstrate this, a defendant must manifest a subjective expectation of privacy in the area searched, and his expectation must be one that society would recognize as objectively reasonable. See id. A defendant has the burden of establishing that, under the totality of the circumstances, the search or seizure violated his legitimate expectation of privacy. See id.

There is no reasonable expectation of privacy in financial records such as checks, deposit slips, and financial statements maintained by third party institutions such as banks, because a "depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." See In re Grand Jury Proceedings, 40 F.3d 959, 962 (9th Cir. 1994) (citing United States v. Miller, 425 U.S. 435, 442-43 (1976)). This includes records maintained in association with funds deposited into a foreign bank. See id. at 963. Even if information is revealed to a third party on the assumption that it will be used only for a limited purpose and that the confidence placed in the third party will not be betrayed, the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities. See Miller, 425 U.S. at 443.

Therefore, the Court concludes that Plaintiff lacks standing to challenge the evidence collected by the Government from e-gold, including the time and date of Plaintiff's transactions through his e-gold account, his e-gold account number and the account number of the parties with whom he was transacting business, the IP addresses from where the transactions were sent, the amounts paid, and memos documenting the purposes of the transactions, because Plaintiff voluntarily revealed that information to e-gold. See In re Grand Jury Proceedings, 40 F.3d at 962-63 ("Where an individual's Fourth Amendment rights are not implicated, obtaining the documents does not violate his or her rights, even if the documents lead to indictment."). Accordingly, the Court denies Plaintiff's motion to suppress the evidence obtained on the basis of evidence the

Government received from e-gold.

II. 18 U.S.C. § 2703

The Court also concludes that the Government did not violate 18 U.S.C. § 2703(a)[2] by utilizing an administrative subpoena to gather information from e-gold because e-gold is not a provider of electronic communication services. Pursuant to § 2703(a), a governmental entity may only require the disclosure of the contents of an electronic communication that is in electronic storage in an electronic communications system for 180 days or less from a provider of electronic communication service pursuant to a warrant by a court with jurisdiction over the offense under investigation or pursuant to an equivalent state warrant. An "electronic communication service," as defined by 18 U.S.C. § 2510(15),[3] means "any service which provides to users thereof the ability to send or receive wire or electronic communications." An "electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include– (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds." 18 U.S.C. § 2510(12).

The Court concludes that e-gold is not a service which provides users the ability to send or receive electronic communications, rather e-gold is a service which utilizes the ability to send or receive electronic communications to permit the instant transfer of gold ownership between its users. See In re U.S. for an Order Authorizing Roving

---

[2] Section 2703 is part of the Stored Communications Act, 18 U.S.C. §§ 2701-2711, which was passed by Congress as Title II of the Electronic Communications Privacy Act of 1986. See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).

[3] Pursuant to 18 U.S.C. § 2711(1), 18 U.S.C. § 2510 provides the applicable definitions for the Stored Communications Act.

Interception of Oral Communications, 349 F.3d 1132, 1140 (9th Cir. 2003) (defining the term "provides" in § 2510 as it would be used "in ordinary discourse," and therefore finding that a company that billed and had direct dealings with customers for communication services was the provider of those services); see also Crowley v. Cybersource Corp., 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001) (concluding Amazon.com, Inc., which does not independently provide electronic communication service to the public, was not a provider, but rather a user, of electronic communication service, even though it could communicate with customer's through e-mail); S. Rep. No. 99-541, at 14 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3568 ("[T]elephone companies and electronic mail companies are providers of electronic communication services."); cf. United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993) (airline that provides travel agents with computerized travel reservation system accessed through separate computer terminals can be a provider of electronic communication service). Therefore, the Government was not required by § 2703(a) to utilize a warrant to obtain the requested information from e-gold.

Similarly, Defendant's argument that the Government exceeded the permitted scope of a request for information pursuant to an administrative subpoena based on § 2703(c)(2)[4] fails because e-gold is neither a provider of electronic communication service or a remote computing service. The Court has already concluded that Defendant is not a provider of electronic communication service.

The term "remote computing service" is defined by 18 U.S.C. § 2711(2) as the "provision to the public of computer storage or processing services by means of an electronic communications system." The Senate explained the term "remote computing service," as used in the Stored Communications Act:

/ / /

[4] An administrative subpoena issued to a provider of electronic communication service or remote computing service regarding a federal offense involving the sexual exploitation or abuse of children may not extend beyond requiring the provider to disclose the information specified in 18 U.S.C. § 2703(c)(2). See 18 U.S.C. § 3486(a)(1)(C)(i).

> In the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data inhouse on the user's own computer or on someone else's equipment. Over the years, remote computer service companies have developed to provide sophisticated and convenient computing services to subscribers and customers from remote facilities. Today businesses of all sizes--hospitals, banks and many others--use remote computing services for computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer. Data is most often transmitted between these services and their customers by means of electronic communications.

S. Rep. No. 99-541, at 10-11 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3564-64.

The Court concludes that e-gold provides neither computer storage nor processing services, as those terms are used in § 2711(2), to the public. Cf. Quon v. Arch Wireless Operating Co., Inc., 445 F. Supp. 2d 1116, 1130-37 (C.D. Cal. 2006) (concluding that wireless communications provider that stored and retrieved text messages for its subscribers was a remote computing service); Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it, 72 Geo. Wash. L. Rev. 1208, 1229-30 (2004) (concluding that eBay is not a remote computing service because "[t]he legislative history indicates that 'processing services' refer to outsourcing functions. . . . This seems quite different from eBay: a user does not outsource tasks to eBay but rather uses eBay as a destination for the user's requests concerning buying and selling items."). A client of e-gold does not outsource tasks, but rather uses e-gold to transfer gold ownership to other users. Neither does an e-gold customer use e-gold to simply store electronic data. Accordingly, the Court also denies Defendant's motion to suppress evidence obtained on the basis of information the Government received from e-gold because the Government did not violate 18 U.S.C. § 2703(a) or § 2703(c)(2).

III. Probable Cause

Defendant argues that even if the information the Government obtained from e-gold was not illegally obtained, the evidence collected from Defendant's home should be suppressed because the issued warrant lacked probable cause. "[P]robable

cause means a 'fair probability' that contraband or evidence is located in a particular place." United States v. Kelley, 482 F.3d 1047, 1050 (9th Cir. 2007). Whether there is a fair probability to search a computer for evidence of child pornography depends upon the totality of the circumstances, including reasonable inferences, and is a commonsense, practical question. See id. at 1048, 1050. "Neither certainty nor a preponderance of the evidence is required." Id. at 1050.

A magistrate judge's determination that probable cause exists should be paid great deference. See United States v. Gourde, 440 F.3d 1065, 1069 (9th Cir. 2006). "This deferential approach is the antithesis of a 'grudging or negative attitude' toward search warrants and 'a hypertechnical rather than a commonsense' analysis." Id.

The Court concludes that SA Johnson's affidavit raised a fair probability that evidence was located at Defendant's house demonstrating violations of 18 U.S.C. § 2252. Among the evidence considered by the Court is that the three IP addresses associated with payments to e-gold accounts linked to child pornography websites were from a computer located at Defendant's address and the websites to which subscriptions were purchased have names associated with child pornography. Defendant's argument that there was no evidence cited that any images were actually downloaded from these sites, and that the affidavit relied on an assumption that all imagery from these websites, including any imagery downloaded, was pornographic, is simply an impermissible attempt to elevate the probable cause to a test of near certainty. See Gourde, 440 F. 3d at 1072-73. Accordingly, the Court denies Defendant's motion to suppress the evidence taken from his home based on a lack of probable cause.

/ / /

/ / /

/ / /

/ / /

/ / /

Conclusion

For the reasons discussed, the Court **DENIES** Defendant's motion to suppress evidence seized from his home.

IT IS SO ORDERED.

DATED: August 8, 2007

MARILYN L. HUFF, District Judge
UNITED STATES DISTRICT COURT

COPIES TO:
All parties of record.